AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claims 1-19 (Canceled)

Claim 20 (Currently Amended) A modular arithmetic apparatus, comprising:

a plurality of product-sum circuits configured to ~~input~~ receive a plurality of base elements and execute a modular arithmetic operation; and

a correction term calculation unit configured to ~~input~~ receive ~~the~~ said plurality of base elements in parallel to said plurality of product-sum circuits and to calculate a sequence of bits of a correction term to be used ~~for~~ in said modular arithmetic operation ~~in the product-sum circuits~~, wherein

said correction term calculation unit sequentially calculates the correction term in units of bits, each bit from said sequence being fed to said modular arithmetic operation individually for a corresponding sequential calculation, and

each of said product-sum circuits sequentially ~~reflects~~ uses the correction term calculated by said correction term calculation unit and performs one of a base conversion operation or base extension operation.

Claim 21 (Original) An apparatus according to claim 20, wherein said product-sum circuit performs a Montgomery multiplication.

Claim 22 (Currently Amended) An apparatus according to claim 20, wherein

~~said correction term calculation unit sequentially calculates the correction term in units of bits, and~~

each of said product-sum circuits sequentially reflects the correction term calculated by said correction term calculation unit and converts a residue number system representation into a radix representation.

Claim 23 (Original) An apparatus according to claim 20, wherein said correction term calculation unit comprises a division circuit, and

a base of a residue number system processed by said product-sum circuit is approximated to a power of 2.

Claim 24 (Currently Amended) An apparatus according to claim 20, further comprising:

a bit selection section configured to select an upper bit of said plurality of base elements~~the input to~~ received by said correction term calculation unit.

Claim 25 (Currently Amended) An apparatus according to Claim 20, further ~~comprise~~ comprising:

an I/O section for inputting/outputting data to/from an external unit.